# Ben's Guide to protecting Filesharers from going to prison

## also known as the inventor of the BitTor idea, and known as "Mr. Leader" on Torrentfreak

Thanx torrentfreak, and all filesharing networks for being strong.

I decided to make this guide after this on torrentfreak: **Police Extend OiNK's Bail Date and Returns Servers, Wiped!**

Written by Ernesto on December 07, 2007

The OiNK servers that were raided in October have been returned to OiNK's ISP. **Strangely enough all the data, and thus the evidence, has been wiped**. In addition, the bail date for OiNK admin Alan Ellis, who was arrested during the raid, has today been extended until the 4th of February 2008.

OiNK's Bail ExtendedThe initial bail date was December 21, it is not clear what the reason for the extension is, but , but it is likely that **the police don't have the strong evidence they would like to have**.

In fact, **the police returned the servers last week, not before deleting all the "evidence" that it held**. The police made images of the servers, but it is doubtful if **destroying OiNK's property, and the original evidence is even legal**.

The British and the Dutch police both contributed to what they named "Operation Ark Royal", allegedly acting upon twisted information fed to them by the IFPI and the BPI, two well known anti-piracy organizations.

Among other things, the police claimed that OiNK was a money machine, and that Alan was making hundreds of thousands of pounds. However, everyone knows that OiNK was free to use and this fact was backed up by Trent Reznor, the frontman of Nine Inch Nails: "If OiNK cost anything, I would certainly have paid, but there isn't the equivalent of that in the retail space right now."

The IFPI and BPI did not only misinform the police, they also hijacked the OiNK.cd domain and displayed an ominous message indicating an investigation into the site's users had begun. These propagandistic threats were supposed to scare former OiNK members, and they succeeded in this until OiNK reclaimed the domain.

What once was the best BitTorrent music tracker on the Internet is now gone and wont return. Although most of its members and releasing talent found a new homes by now, there is little doubt that the music industry will continue to alienate itself from their customers until they are dead and gone.

For those who want to help Alan out, there is an official OiNK legal defense fundraiser where money can be donated to cover the legal costs. If for some reason the money isn't needed it will be donated to an animal charity. At this point it is still unclear what the charges against Alan will be, if there will be any at all.

Stay tuned.

---

After this I've decided to release a torrent file with powerful erasing software, and privacy tools to keep the police out of your filesharing/downloading business and keep downloaders and sharers out of prison.

I have studied some law enforcement tactics and they cannot convict you if you have no evidence, such as erasing your computer then reinstalling the operating system and use it like you did before so when cops confiscate your Computers they have no evidence to convict you of copyright infringement.

They can kidnap british citizens, extradite filesharers from Canada, and probably Mexico, but if your computers erased and you used firewalls when you shared they might not be able to convict you.

I also recommend you use your own open Wi-Fi so that the cops will think the filesharers used your Wi-Fi, trying to not get caught and your record will be swept clean.

But here are the main valuable tips cops and lawyers wouldn't want you to get:

**(1)**Until you get a Subpoena you Can erase/destroy the evidence, once you get a Subpoena if you attempt to destroy evidence you can get charged with Obstruction Of Justice and Tampering with evidence.

**(2)**If your not accused of terrorism you cannot let police cops into your home until they have a search warrant. Always keep your computer away from your parents, family, roomates, and Wife because they can consent police to a search of your computer.

**(3)**If you use encryption I recommend you use TrueCrypt because it uses AES Encryption, in fact you can use three encryption schemes such as AES, Twofish, and Serpent together. Cops can't force you to open the encryption container, unless they Use tactics such as torture, torture camps, Tasers, or Waterboarding, if that happens use the Hidden Volume function so you can show the police your not a filesharing/downloading criminal so then your free to go.

**(4)**Always try to encrypt your DATA, wether you use Tor, Hotspot Shield, SSH Services, Anonymous Proxy Services that guarentee your privacy that way cops can't spy on yout traffic without using heavy encryption breakers which might desturb and mess up the internet ruining our economy as we know it so they have to let you use encrypted traffic.

**(5)**When sharing a file to further protect yourself from prosecution share until you get at least 2 or 3 seeds then immedately stop seeding, then your IP Address will be taken off of other peers lists, it's not bulletproof but can further protect you from prosecution.

**(6)**You could also use Tor or a truthworthy proxy to upload to file hosting sites like Mediafire, megaupload, rapidshare, mytempfile, or any other free hosting sites and share your data through there and post to warez sites, under proxy protection, that way your sharing IP will never be revealed.

**(7)** You could possibly use Tor for Bittorrent because you can host hidden services so you could share anonymously through Tor using hidden services:

In your Torrc file you see these configurations:

```
############### This section is just for location-hidden services ###

## Once you have configured a hidden service, you can look at the
## contents of the file ".../hidden_service/hostname" for the address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x to the
## address y:z.

#HiddenServiceDir C:\Documents and Settings\Application Data\Tor
\hidden_service/
#HiddenServicePort 80 127.0.0.1:80

#HiddenServiceDir C:\Documents and Settings\Application Data\Tor
\other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22

ok now we are gonna do some tweaking:

Say you use port 17492 for seeding to peers, in english that means
sharing to people using bittorrent.

#HiddenServiceDir C:\Documents and Settings\Application Data\Tor
\hidden_service/
HiddenServicePort 17492 127.0.0.1:17492

So this is what you change in your torrc file.

I'm not sure if you have to also do HiddenServiceDir, if you do ask
anyone who knows about Tur for help but whatever you do don't tell them
your gonna use Bittorrent as a hidden service, otherwise they will
refuse to tell you anything but Filesharing is wrong, and all that bla
bla bla BS.
```

**(8)** Always erase the free space of your hard drive every week or two times a week to prevent cops from finding deleted data. Also always erase your cache, cookies, MRU, and other tracks every day.

**(9)** If you have a suspicion a police cop is going after you always get a small-as-it-can-be external hard drive and store all your computers data, then erase your computer, with over 10 overwrites, then restore your computer with a legally purchased operating system or restore disk, install tons of freeware and legal software, then hide the drive in an area the cops would never search, I recommend you put it in a waterproof-fireproof lockbox and burry it where your neighbors can't see you, or hide it underground and when the cops go through your door, they will only find a working computer, no copyright infringement, they search through your house, no evidence, and they cannot convict you of a crime, and also remember use a Wi-fi and tell the cops you can't control the airwaves and you try to warn people to use your Wi-fi legally, and then your off the hook.

**(10)** Always try to share at time when lots of people are sharing because it is less likely a spy would pick your your shared file and collect your IP.

**(11)** Anytime you wanna throw away a disk, don't do it because the FBI has been known to search through peoples trash cans, so always shred your DVD or CD, hammer the top pieces and bottom pieces of the disk after you shred it, put black marks on the data area, then throw it in a fire, if theres no fire drown it in acid, if that doesn't work or if you don't have acid use large scissors on a whole disk and cut it(not recommend), or the shredded parts of the disk (recommended) and cut the shredded pieces to even smaller pieces and making recovery or police forensic scans impossible, if it's a RW use full erase, or you could a blow torch on it.

For more info on how to destroy a disk goto: http://www.wikihow.com/Destroy-a-CD-or-DVD in fact to keep people from tracking you from going to that website I'll post the guide here :)

# How to Destroy a CD or DVD


Don't just throw away old discs with personal info. Identity thieves flourish on discs like that. Annihilate them.

## Steps

1. There are several office cd shredder machines, that operate much like common paper shredders. The least expensive are around $40.
2. If you don't kill enough CDs to justify a shredder, a heavy pair of scissors can easily cut through a cd or DVD. The reflective foil will crack and flake at the cut line, making a clean splicing impossible. Be careful, as cutting the disc is tough.
3. If you have many discs and don't want to go through the hassle/danger of cutting up or breaking them, the eco-friendly Disc Eraser is available for about $15 online at www.DiscEraser.com.
4. If you are a thuggish sort and want to have a bit of fun, try smashing the offending disc! Wrap the CD or DVD in a towel and then break or crack it with a firm kick or heavy hammer. The towel will protect you as CDs tend to shatter into sharp pieces. Place the broken CD bits into the trash while wearing safety gloves.
5. If you feel kind of crazy, you could place the CD or DVD into a microwave and nuke it for 5 seconds, or until you see sparks along the surface of the disk. When you pull it out, it'll have a spiderweb pattern of cracks. However, this can be dangerous and destroy your microwave (see

the warnings below), so it is not recommended.
6. Put several strips of duct tape over the top of the CD. Once the tape is firmly attached, rip it off. The foil lining should come off and you will be left with a transparent CD. This trick does not work on all CDs.
7. Some discs, especially burned ones, have the data layer unprotected by plastic. In this case, take a table knife to the label and start scraping shiny flakes into a wastebasket.
8. For the more DIY approach a belt sander on the label side. This is quite messy, little flakes all over, so do it in an area that is easy to clean.
9. Take the cd outside and lay it on several layers of aluminum foil then use a blow torch to melt the cd into a puddle of goo. Actually this wastes your precious butane. Just light a small fire with twigs and newspaper and toss it in...
10. If you have the technical background, you could do us all a favor and simply write CD burner software that a) ignores previous data on the CD, and b) writes an entropy file over what was there.
11. or you can do a flying disk!

# Warnings

* Some microwaves could be damaged by a cd. CDs and DVDs contain a small amount of metal. Damage may be avoided or lessened by placing a glass of water in the microwave with the CD.
* The data on the CD or DVD can still be retrieved after microwaving it, but it would take a professional with a lot of resources.
* Nuking a CD or a DVD even for 5 seconds can produce a very bad odor.
* The vapors or fumes released from most DVD's and CD's while microwaving them are TOXIC. Do not do the above unless you have a spare microwave, as the fumes can attach to the walls of the microwave, or cling to your food.
* Blow torches are dangerous and the vapors are TOXIC. Stay as far from the cd as you can while you burn it and avoid inhaling the fumes. Wear gloves and safety goggles and have a bucket of water handy just in case.
* Due to the nature of some methods, children and irresponsible adults should not attempt to destroy a disc.
* People with professional tools may still be able to read fragments of CDs, so be sure to damage the surface, not just shatter the CD.

# Things You'll Need

* Towel
* Safety Glasses
* Gloves
* Hammer - Optional
* Blow torch - Optional

Ok now you got a lot of tips, Now I won't share any more until the next version of this guide, thats right I will keep making changes and updates since the laws can change, technology can change, products and services can change, filesharing protocols can change, well Thanks for reading this and I hope I gave you enough information on how to stay out of trouble while filesharing/downloading :) 0:)

thanks and have a great day!